UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1	7503

46583 7590 09/18/2007

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER	
SCHMIDT, KARI L	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
09/18/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

gbpatent@gbpatent.com
pto@gbpatent.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,119	BUNN ET AL.	
	Examiner	Art Unit	
	Kari L. Schmidt	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 06/28/2007. Claims 1-20 remain pending. Claims 12-20 have been added.

Response to Arguments

Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Bunker, V et al. (US 2003/0028803 A1).

Claim 1

Bunker discloses a method for checking network perimeter security, said method comprising the steps of: reviewing security of a network perimeter architecture; reviewing security of data processing devices that transfer data across the perimeter of the network; reviewing security of applications that transfer data across said perimeter; and reviewing vulnerability of applications or data processing devices within said

perimeter from computers or users outside of said perimeter; and generating a report concerning security of said perimeter based upon all of the reviewing steps (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0012]: " the preferred embodiment includes a test center and one or more testers. The functionality of the test center may be divided into several subsystem components, possibly including a database, a command engine, a gateway, a report generator, and early warning generator and a repository master copy.").

Claim 2

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter (see at least, [0122]: "Each Tester 502 may be pre-configured in-house and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in the field. An exception might be an out-of-band, dial-up modem that might feature strong encryption for authentication, logging, and dial-back capabilities to

limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0125]: "Any username and password combination is susceptible to compromise, so an alternative is to not use passwords. An option is that only the administrator account has a password and that account can only be logged on locally (and not for example through the Internet) via physical access or the out-of-band modem. In this scenario, all other accounts have no passwords. Access would be controlled by means of public/private key technology that provides identification, authentication, and non-reputability of the user.").

Claim 3

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of data processing devices that authorize computers or users outside of said perimeter that request to access an application within said perimeter (see at least, [0122]: "Each Tester 502 may be pre-configured in-house and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in the field. An exception might be an out-of-band, dial-up modem that might feature

strong encryption for authentication, logging, and dial-back capabilities to limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0123]: "Until the integrity of Tester 502 may be verified by an outside source, it may be the case that no communication with the device will be trusted and the device may be marked as suspect. Confidence in integrity may be improved by several means. First of all, Tester's 502 arsenals of tools 514, both proprietary and open source, may be contained on encrypted file systems. An encrypted file system may be a "drive" that, while unmounted, appears to be just a large encrypted file. In that case, when the correct password is supplied, the operating system would mount the file as a useable drive. The may prevent for example an unauthorized attacker with physical access to the Tester 502 from simply removing the drive, placing it into another machine and reading the contents. In that case, the only information an attacker might have access to might be the standard build of whatever operating system the Tester 502 happened to be running. If used, passwords may be random, unique to each Tester 502, and held in the Test Center 102. They may be changed from time to time, for example, on a bi-weekly basis.").

Claim 4

Bunker discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of a web server, an e-mail server or an FTP server (see at least, [0116]-[0117], [0175]: "For the purposes of an internal assessment, several different appliances may be deployed on the customers network 1002. For example, for traveling consultants, a pre-configured laptop computer loaded with an instance of a Tester 502 might be shipped for deployment. For permanent, continuous assessment installations a dedicated, pre-configured device in either a thin, rack mountable form or desktop style tower might be shipped for deployment. In both cases the device might boot out-of-the-box to a simple, graphical, configuration editor. The editor's interface is a web browser that might point to the active web server on the local loop-back device. Since the web server may be running on the loop-back device, it may only be accessible by the local machine. Some options of local configurations might include, for example: IP Stack configuration, DNS information, default route table, push/pull connection to Test Center 102, account information, etc. Other options in the local configuration might include for example: IP diagnostics (Ping, Trace Route, etc.), DNS Resolutions, connections speed, hardware performance graphs, etc.")[0181] Overview 1400 in FIG. 14 illustrates a sample of the attack logic used by the preferred embodiment. Prior to the first "wave" 1410 of basic tests 516, an initial mapping 1402 records a complete inventory of services running on the target network 1002. An initial mapping 1402 discloses what systems 1102 are

present, what ports are open (1404, 1406, and 1408) what services each system is running, general networking problems, web or e-mail servers, whether the system's IP address is a phone number, etc. Basic network diagnostics might include whether a system can be pinged, whether a network connection fault exists, whether rerouting is successful, etc. For example, regarding ping, some networks have ping shut off at the router level, some at the firewall level, and some at the server level. If ping doesn't work, then attempt may be made to establish a handshake connection to see whether the system responds. If handshake doesn't work, then request confirmation from the system of receipt of a message that was never actually sent because some servers can thereby be caused to give a negative response. If that doesn't work, then send a message confirming reception of a message from the server that was not actually received because some servers can thereby be caused to give a negative response. Tactics like these can generate a significant amount of information about the customer's network of systems 1002.").

Claim 5

Bunker discloses the method as set forth in claim 1 further comprising the step of reviewing security of a server within said perimeter that provides data to said data processing devices that transfer data across the perimeter of said network (see at least, [0048] Database Subsystem Functionality; [0059], [0049]: "The Database 114 has multiple software modules and storage facilities 200 for performing different functions. The Database warehouses the raw data 214 collected by the Testers' 502 tests 516

from customers systems and networks 1002 and that data may be used by the Report Generator 112 to produce different security reports 2230 for the customers. The raw data contained in the Database 114 can be migrated to any data format desired, for example by using ODBC to migrate to Oracle or Sybase. The type of data might include, for example, IP addresses, components, functions, etc. The raw data 214 may typically be fragmented and may not be easily understood until decoded by the Report Generator 110." [0052]: " The job scheduling module can initiate customer jobs at any time. It uses the customer profile information to tell the Command Engine what services the customer should receive, due to having been purchases, so that the Command Engine can conduct the appropriate range of tests." [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc.").

Claim 6

Bunker discloses the method as set forth in claim 1 wherein each of said reviews is performed by comparison to a security policy of an enterprise which owns or controls said network (see at least, [0059], [0149], [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0019] When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the

customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.").

Claim 7

Bunker discloses the method as set forth in claim 1 further comprising the step of determining said network perimeter (see at least, [0003], [0006], [0009], [0010], [0011]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations.").

Claim 8

Bunker discloses the method as set forth in claim 7 wherein said network perimeter comprises entries and exits from said network (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly

complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0059]: "The ability to perform performance metrics 208 comes from two places: (1) utilizing standard network utilities and methodologies, and (2) analysis of database 114 information. More sources of the ability to perform performance metrics 208 will become available over time. Current performance metrics 208 include, job completion timing, which is (1) time to complete an overall assessment (can be compared with type of assessment as well as size of job); (2) time to complete each Tool Suite 9 e.g., HTTP Suite 2318); (3) time to complete each wave of tests 516; and (3) time to complete each test 516. Also, assessment time per IP address/active nodes assessment time per type of service active on the machine. Tester 502 performance metrics 208 include, for example, resources available/used, memory, disk space, and processor. Gateway 118 performances metrics 208 include, for example, resources available/used, memory, disk space, and processor. Other performance metrics 208 include, for example, communication time between Tester 502 and Gateway 118 (latency), communication time between Gateway 118 and Tester 502 (network paths are generally different), and bandwidth available between Tester 502 and Gateway 118. Future performance metrics might include, Tester 502 usage, by operating system, by Network (Sprint, MCI, etc.), IP address on each Tester 502; test 516 effectiveness by operating system, by Network, by Tester 502; and Gateway

118/Distribution of tests across Testers 103."; [0100], [0095], [0094], [0116], [0122], [0126]: "Security typically requires vigilance. Several processes may be in place to improve awareness of malicious activity that may be targeting an embodiment fo the invention. Port Sentries and Log Sentries may be in place to watch and alert of any suspicious activity and as a host-based intrusion detection system. Port Sentry is a simple, elegant, open source, public domain tool that is designed to alert administrators to unsolicited probes. Port sentry opens up several selected ports and waits for someone to connect. Typical choices of ports to open are services that are typically targeted by malicious attackers (e.g., ftp, sunRPC, Web, etc.). Upon connection, the program may do a variety of different things: drop route of the attacker to /dev/nul; add attacker to explicit deny list of host firewall; display a strong, legal warning; or run a custom retaliatory program. As such a strong response could lead to a denial of service issue with a valid customer, an alternative is to simply use it to log the attempt to the Tester 502 logs. Log sentry is another open source program that may be utilized for consolidation of log activity. It may check the logs every five minutes and email the results to the appropriate Internet address." [0181]).

Claim 9

Bunker discloses the method as set forth in claim 1 wherein said network perimeter comprises entries and exits from said network (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly

complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0059]: "The ability to perform performance metrics 208 comes from two places: (1) utilizing standard network utilities and methodologies, and (2) analysis of database 114 information. More sources of the ability to perform performance metrics 208 will become available over time. Current performance metrics 208 include, job completion timing, which is (1) time to complete an overall assessment (can be compared with type of assessment as well as size of job); (2) time to complete each Tool Suite 9 e.g., HTTP Suite 2318); (3) time to complete each wave of tests 516; and (3) time to complete each test 516. Also, assessment time per IP address/active nodes assessment time per type of service active on the machine. Tester 502 performance metrics 208 include, for example, resources available/used, memory, disk space, and processor. Gateway 118 performances metrics 208 include, for example, resources available/used, memory, disk space, and processor. Other performance metrics 208 include, for example, communication time between Tester 502 and Gateway 118 (latency), communication time between Gateway 118 and Tester 502 (network paths are generally different), and bandwidth available between Tester 502 and Gateway 118. Future performance metrics might include, Tester 502 usage, by operating system, by Network (Sprint, MCI, etc.), IP address on each Tester 502; test 516 effectiveness by operating system, by Network, by Tester 502; and Gateway

118/Distribution of tests across Testers 103."; [0100], [0095], [0094], [0116], [0122], [0126]: "Security typically requires vigilance. Several processes may be in place to improve awareness of malicious activity that may be targeting an embodiment fo the invention. Port Sentries and Log Sentries may be in place to watch and alert of any suspicious activity and as a host-based intrusion detection system. Port Sentry is a simple, elegant, open source, public domain tool that is designed to alert administrators to unsolicited probes. Port sentry opens up several selected ports and waits for someone to connect. Typical choices of ports to open are services that are typically targeted by malicious attackers (e.g., ftp, sunRPC, Web, etc.). Upon connection, the program may do a variety of different things: drop route of the attacker to /dev/nul; add attacker to explicit deny list of host firewall; display a strong, legal warning; or run a custom retaliatory program. As such a strong response could lead to a denial of service issue with a valid customer, an alternative is to simply use it to log the attempt to the Tester 502 logs. Log sentry is another open source program that may be utilized for consolidation of log activity. It may check the logs every five minutes and email the results to the appropriate Internet address." [0181]).

Claim 10

Bunker discloses the method as set forth in claim 1 wherein the steps of reviewing security of a network perimeter, reviewing security of data processing devices that transfer data across the perimeter of the network, and reviewing vulnerability of applications or data processing devices within said perimeter from entities outside of

said perimeter are performed at least in part with a respective program tool (see at least, [0010]: "the preferred embodiment provides real-time network security vulnerability assessment tests, possibly complete with recommended security solutions, external vulnerability assessment tests may emulate hacker methodology in a safe way and enable study of a network for security openings, gaining a true view of risk level without affecting customer operations. This assessment may be performed over the internet for domestic and worldwide corporations." [0012]: " the preferred embodiment includes a test center and one or more testers. The functionality of the test center may be divided into several subsystem components, possibly including a database, a command engine, a gateway, a report generator, and early warning generator and a repository master copy." [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0019] When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library

enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.").

Claim 11

Bunker discloses the method as set forth in claim 1 wherein the step of reviewing security of said data processing devices comprises the step of reviewing security of data processing devices accessed by users outside of said perimeter (see at least, [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc.

The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0122]: "Each Tester 502 may be pre-configured in-house and designed for remote administration. Therefore, it may be that no peripherals (e.g., keyboard, monitor, mouse, floppies, CD-ROM drives, etc.) are enabled while the Tester 502 is in the field. An exception might be an out-of-band, dial-up modem that might feature strong encryption for authentication, logging, and dial-back capabilities to limit unauthorized access. This modem may be used, for example, in emergencies when the operating system is not completing its bootstrap and may be audited on a continuous basis. This may limit the need for "remote-hands" (e.g., ISP employees) to have system passwords, and may reduce the likelihood of needing a lengthy on-site trip. Other physical security methods, such as locked computer cases, may be implemented. One example might be a locked case that would, upon unauthorized entry, shock the hardware and render the components useless." [0125]: "Any username and password combination is susceptible to compromise, so an alternative is to not use passwords. An option is that only the administrator account has a password and that account can only be logged on locally (and not for example through the Internet) via physical access or the out-of-band modem. In this scenario, all other accounts have no passwords.

Access would be controlled by means of public/private key technology that provides identification, authentication, and non-reputability of the user.).

Claim 12

Bunker discloses the method as set forth in claim 1, wherein the reviewing security of data processing devices that transfer data across the perimeter of the network comprises categorizing components as either control points or non-control points (see at least, [0073]).

Claim 13

Bunker discloses the method as set forth in claim 12, wherein the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises: testing control points with port scans; and testing control points with penetration tests (see at least, [0094-0095])

Claim 14

Bunker discloses the method as set forth in claim 1, further comprising: performing a policy review of an enterprise which owns or controls said network; defining review parameters based upon the policy review; and utilizing the review parameters to perform each of: the reviewing security of a network perimeter architecture, the reviewing security of data processing devices that transfer data across the perimeter of the network, the reviewing security of applications that transfer data across said

perimeter, and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter (see at least, (see at least, [0010-0012], [0059], [0149], [0054]: "Every customer has a customer profile that may include description of the services the customer will be provided, the range of IP addresses the customer's network spans, who should receive the monthly reports, company mailing address, etc. The customer profile may be used by the Command Engine to conduct an appropriate set of tests on the customer's systems. The customer profile may be also used by the Report Generator to generate appropriate reports and send them to the appropriate destination. Customer Profile information includes that information discussed in this specification which would typically be provided by the Customer, such as IP addresses, services to be provided, etc." [0019] When a new security vulnerability may be announced on a resource like Bugtraq, the information may be added to the Vulnerability Library. Each vulnerability may be known to affect specific types of systems or specific versions of applications. The Vulnerability Library enables each vulnerability to be classified and cataloged. Entries in the Vulnerability Library might include, for example, vulnerability designation, vendor, product, version of product, protocol, vulnerable port, etc. Classification includes designating the severity of the vulnerability, while cataloging includes relating the vulnerability to the affected system(s) and/or application(s). The configuration of the new vulnerability may be compared to the customer's system network configuration compiled in the last test for the customer. If the new vulnerability is found to affect the customer systems or networks then a possibly detailed alert may be sent to the

customer. The alert indicates which new vulnerability threatens the customer's network, possibly indicating specifically which machines may be affected and what to do in order to correct the problem. Then, depending on the customer profile, after corrective measures are taken, the administrator can immediately use the system to verify the corrective measures in place or effectiveness of the corrective measures may be verified with the next scheduled security assessment.").

Claim 15

Bunker discloses the method as set forth in claim 1, wherein: the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases; the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases; the reviewing security of applications that transfer data across said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases; and the reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter comprises receiving the review parameters, receiving the test cases, and performing the test cases (see at least, [0010-0012], [0054], [0069-0083], [0095]).

Claims 16-20

The computer program product and system claims are one of the same therefore rejected for the same reason as the method claims 1-15 above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wiegel (US 6,484,261 B1) teaches graphical network security policy management.

Kurtz et al. (US 2003/0217039 A1) teaches systems and method for network vulnerability detection and reporting.

Bunker, V et al. (US 2003/0056116 A1) teaches reporter.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100